SPECIFICATION AMENDMENTS

Please add the following new paragraph after existing paragraph [90] at line 21 on page 24:

[90.1] In step 420, a second set of computations involving multiplicative inverses modulo prime moduli p1, p2, etc., is substituted. For example, a first set of computations that involves the multiplicative inverse modulo moduli m1, m2, etc. is substituted with a second set of computations modulo prime moduli p1, p2, etc., according to expression (23).